CLAIMS

1. A home server including a proxy facility provided between a user terminal and an electronic market server for executing authentication and encryption to the electronic market server, instead of the user terminal, in an electronic commercial transaction, comprising:

an establishing means for establishing an encrypted communication session between the user terminal and the home server, using public/secret keys of the user terminal and an electronic signature both transmitted from the user terminal;

a proxy means for executing authentication of a certificate and exchanging a common key between the home server and the electronic market server, using public/secret keys of the electronic market server; and

an information means for informing the common key to the user terminal through the encrypted communication session;

wherein an encrypted communication is executed between the user terminal and the electronic market server by using the common key that was exchanged between the home server and the electronic market server.

2. A home server including a proxy facility as claimed in claim 1, further comprising a home card including an encryption managing means for executing the electronic signature and authentication of the certificate in order to execute authentication and exchange of the common key to the electronic market server.

3. A home server including a proxy facility as claimed in claim 2, wherein the home card includes a logic circuit which enables an access by using a first password input from the user terminal; and a security releasing means for releasing the security for the proxy means by using a second password input from the user terminal, after establishment of the encrypted communication session to the user terminal in which an

access was permitted,

4. A home server including a proxy facility as claimed in claim 2, wherein the home card comprises an information means for recording decision information regarding an electronic money in the home card and for informing the recorded decision information to a mail address of the user terminal.

5. A home server including a proxy facility as claimed in claim 4, wherein the home card comprises a cancel means for canceling the decision information in the home card based on an authentication information for canceling the decision, and for adding electronic money subtracted by the decision to the electronic money in the home card.

6. A home server including a proxy facility as claimed in claim 2, wherein the home card comprises a re-supplement means for supplementing the electronic money by adding supplementary electronic money, which was requested by the user terminal, to the electronic money in the home card, based on the authentication information in an electronic money managing facility provided in the proxy facility.

7. An access card used in an electronic commercial transaction constituted by a user terminal, a home server and an electronic market server; the access card being connected to the user terminal; and the home server including a proxy facility being provided between the user terminal and the electronic market server for executing authentication and encryption to the electronic market server, instead of the user terminal; the access card comprising:

an establishment means for establishing an encrypted communication session between the user terminal and the home server including the proxy facility; and

an encrypted communication means for receiving a common key, which is exchanged between the home server and the electronic market server after an authentication process for the electronic market server, from the home server through the encrypted communication session, and for executing the encrypted communication with the electronic market server by using the common key.

8. A server being able to communicate with a user terminal and the other server having an authentication facility to authenticate the user terminal in accordance with predetermined procedures in an electronic commercial transaction, comprising:

a reception unit to receive an identification information and a request for executing an authentication process, from the user terminal;

a decision means for determining whether or not the identification information is stored in an internal or external memory; and

a proxy means for executing a part, or all, communication in accordance with the predetermined procedures when the identification information is stored in the memory.

9. A storage media storing a predetermined program used in a first server being able to communicate with a user terminal and a second server having an authentication facility to authenticate the user terminal in accordance with predetermined procedures in an electronic commercial transaction, comprising:

a first step of receiving an identification information and a request for executing an authentication process, from the user terminal;

a second step of determining whether or not the identification information is stored in an internal or external memory; and

a third step of executing a part, or all, communication in accordance with the predetermined procedures when the identification information is stored in the memory.

10. A user terminal being able to communicate with

a first server and a second server;

wherein the first sever includes a proxy facility for executing authentication with the second server instead of the user terminal, when receiving an identification information and a request for executing an authentication process from the user terminal; and the second server has an authentication facility to authenticate the user terminal in accordance with predetermined procedures and to provide a secret key for an authorized destination as a result of authentication; and

wherein the user terminal comprises a transmitting unit to transmit the identification information used for identifying its own terminal and the request for executing the authentication process, to the first server, and a receiving unit to receive the secret information from the first server.